Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (previously presented) A method for discovering a trust chain, wherein the trust chain comprises at least attribute delegations each with an issuer and a subject, overall imparts a required attribute to a subject, and is grounded in a known trusted issuer, and wherein certificates are used as justification of associated attribute delegations, the method comprising:

a) setting as a primary goal to be proved an attribute delegation from a known trusted issuer to said subject;

b) seeking a backwards proof of said primary goal by a process of recursively taking a goal to be proved, starting with said primary goal, and decomposing it into subgoals one of which corresponds to an attribute delegation that is justified by an available certificate and has the same subject as the goal being decomposed, inability to decompose a subgoal that has not been proved causing the process to backtrack to a previous subgoal to seek a new decomposition of the latter; and

c) determining that a trust chain has been found upon the process of (b) producing a chain of subgoals that is proved by corresponding certificates and that grounds in a subgoal justified by a justified attribute delegation that has as issuer the said known trusted issuer included in said primary goal.

2. (previously presented) A method according to claim 1, wherein the known trusted issuer included in said primary goal is a specifically identified entity that is inherently trusted by the discovery method at least in relation to said required attribute, said justified attribute delegation being an attribute delegation that is justified by a corresponding certificate.

3. (previously presented) A method according to claim 1, wherein the known trusted issuer included in said primary goal is the discovery method itself; said justified attribute delegation being an attribute delegation that is justified either by an axiom inherently trusted by the discovery method, or by a corresponding certificate.

4. (original) A method according to claim 3, wherein the discovery method, as said known trusted issuer, is represented in said primary goal and said axiom as a null issuer.

5. (previously presented) A method according to claim 1, wherein name mappings justified by corresponding certificates are permitted in a said trust chain in addition to attribute delegations, and wherein the process of (b) further comprises:

decomposing, as appropriate, a particular subgoal to be proved into a name mapping justified by an available certificate and a new subgoal corresponding to said particular subgoal but with the subject reverse mapped using said name mapping.

6. (previously presented) A method according to any one of the preceding claims, wherein seeking a backwards proof further comprises:

maintaining a list of subgoals already generated and pursued, checking each new subgoal against said list, and terminating the process of seeking of a backwards proof in failure in the event of a new subgoal being found to already exist in the list.

7. (currently amended) A method according to any one of ~~the preceding~~ claims 1-5, wherein at least some of said certificates used in proving a determined trust chain as found have associated validity data, the method comprising the further step of traversing the trust chain in a forwards direction from the trusted attribute delegation that grounds it and combining the validity data of all certificates involved to determine the validity of the overall attribute delegation represented by the chain.

8. (previously presented) A method according to claim 7, wherein determining that a trust chain has been found comprises storing the state of the seeking of a backwards proof prior to checking the validity of the trust chain found, this state being used to continue the process should the check of the validity of the initially found chain show that the chain is not valid.

9. (currently amended) A method according to any one of ~~the preceding~~ claims 1-5, wherein an attribute-delegation certificate used to prove a said subgoal has a subject-directed condition associated with it requiring that a specified subject must have a particular attribute in order for the delegation to be valid, and wherein the process of (b) further comprises:

making said subject-directed condition a further subgoal to be proved for the current chain being followed.

10. (currently amended) A method according to any one of claims 1-5 ~~claim 1~~, wherein the process of ~~step~~ (b) is run to completion to find all trust chains, if any, proving the primary goal.

11. (currently amended) A method of selecting certificates to be sent to a resource which requires proof that a subject has a particular attribute before allowing use of the resource, comprising:

finding a trust chain by the method of any one of claims 1 to [[7]] 5 in respect of said subject and an issuer known, or likely, to be trusted by said resource; and

selecting for sending to said resource certificates associated with a trust chain, if any, thereby found.

12. (currently amended) A method of determining whether a resource requiring a user to have at least one predetermined

attribute, is usable by a subject presenting certificates to the resource, comprising:

finding a trust chain by the method of any one of claims 1 to [[7]] 5 in respect of said subject and an issuer known and trusted by said resource; and

determining that use of the resource by the subject is permitted if a trust chain can be found.

13. (previously presented) A system for discovering a trust chain, wherein the trust chain comprises at least attribute delegations each with an issuer and a subject, overall imparts a required attribute to a subject, and is grounded in a known trusted issuer, and wherein certificates are used as justification of associated attribute delegations, the system comprising a processor for:

setting as a primary goal to be proved an attribute delegation from a known trusted issuer to said subject;

seeking a backwards proof of said primary goal by a process of recursively taking a goal to be proved, starting with said primary goal, and decomposing it into subgoals one of which corresponds to an attribute delegation that is justified by an available certificate and has the same subject as the goal being decomposed, inability to decompose a subgoal that has not been proved causing the process to backtrack to a previous subgoal to seek a new decomposition of the latter; and

determining that a trust chain has been found upon producing a chain of subgoals that is proved by corresponding

certificates and that grounds in a subgoal justified by a justified attribute delegation that has as issuer the said known trusted issuer included in said primary goal.

14. (previously presented) A system according to claim 13, wherein the known trusted issuer included in said primary goal is a specifically identified entity that is inherently trusted at least in relation to said required attribute, said justified attribute delegation being an attribute delegation that is justified by a corresponding certificate.

15. (previously presented) A system according to claim 13, wherein the known trusted issuer included in said primary goal is a discovery method of the system itself; said justified attribute delegation being an attribute delegation that is justified either by an axiom inherently trusted by the discovery method, or by a corresponding certificate.

16. (previously presented) A system according to claim 15, wherein the discovery method, as said known trusted issuer, is represented in said primary goal and said axiom as a null issuer.

17. (previously presented) A system according to claim 13, wherein name mappings justified by corresponding certificates are permitted in a said trust chain in addition to attribute delegations, and wherein seeking a backwards proof further

comprises:

decomposing, as appropriate, a particular subgoal to be proved into a name mapping justified by an available certificate and a new subgoal corresponding to said particular subgoal but with the subject reverse mapped using said name mapping.

18. (previously presented) A system according to any one of claims 13-17, wherein seeking a backwards proof further comprises:

maintaining a list of subgoals already generated and pursued, checking each new subgoal against said list, and terminating the process of seeking a backwards proof in failure in the event of a new subgoal being found to already exist in the list.

19. (currently amended) A system according to any one of claims 13-17 ~~18~~, wherein at least some of said certificates used in proving a determined trust chain as found have associated validity data, the processor further for traversing the trust chain in a forwards direction from the trusted attribute delegation that grounds it and combining the validity data of all certificates involved to determine the validity of the overall attribute delegation represented by the chain.

20. (previously presented) A system according to claim 19, wherein determining that a trust chain has been found comprises storing the state of the seeking of a backwards proof prior to

checking the validity of the trust chain found, this state being used to continue the process should the check of the validity of the initially found chain show that the chain is not valid.

21. (currently amended) A system according to any one of claims 13-17 ~~20~~, wherein an attribute-delegation certificate used to prove a said subgoal has a subject-directed condition associated with it requiring that a specified subject must have a particular attribute in order for the delegation to be valid, and wherein seeking a backwards proof further comprises:

making said subject-directed condition a further subgoal to be proved for the current chain being followed.

22. (previously presented) A system according to claim 13, wherein the seeking of a backwards proof is run to completion to find all trust chains, if any, proving the primary goal.

23. (currently amended) A system according to any one of claims 13-17 ~~18~~, wherein said processor is further for selecting certificates to be sent to a resource which requires proof that a subject has a particular attribute before allowing use of the resource by:

finding a trust chain in respect of said subject and an issuer known, or likely, to be trusted by said resource; and

selecting for sending to said resource certificates associated with a trust chain, if any, thereby found.

24. (currently amended) A system according to any one of claims 13-17 ~~18~~, wherein said processor is further for determining whether a resource requiring a user to have at least one predetermined attribute is usable by a subject presenting certificates to the resource, by:

finding a trust chain in respect of said subject and an issuer known and trusted by said resource; and

determining that use of the resource by the subject is permitted if a trust chain can be found.

25. (previously presented) A computer program product for use in connection with a computer for discovering a trust chain, wherein the trust chain comprises at least attribute delegations each with an issuer and a subject, overall imparts a required attribute to a subject, and is grounded in a known trusted issuer, and wherein certificates are used as justification of associated attribute delegations, said computer program product comprising a computer-readable medium having encoded thereon instructions for:

setting as a primary goal to be proved an attribute delegation from a known trusted issuer to said subject;

seeking a backwards proof of said primary goal by a process of recursively taking a goal to be proved, starting with said primary goal, and decomposing it into subgoals one of which corresponds to an attribute delegation that is justified by an available certificate and has the same subject as the goal being

decomposed, inability to decompose a subgoal that has not been proved causing the process to backtrack to a previous subgoal to seek a new decomposition of the latter; and

determining that a trust chain has been found upon producing a chain of subgoals that is proved by corresponding certificates and that grounds in a subgoal justified by a justified attribute delegation that has as issuer the said known trusted issuer included in said primary goal.

26. (previously presented) A computer program product according to claim 25, wherein the known trusted issuer included in said primary goal is a specifically identified entity that is inherently trusted at least in relation to said required attribute, said justified attribute delegation being an attribute delegation that is justified by a corresponding certificate.

27. (previously presented) A computer program product according to claim 25, wherein the known trusted issuer included in said primary goal is a discovery method itself; said justified attribute delegation being an attribute delegation that is justified either by an axiom inherently trusted by the discovery method, or by a corresponding certificate.

28. (previously presented) A computer program product according to claim 27, wherein the discovery method, as said known trusted issuer, is represented in said primary goal and

said axiom as a null issuer.

29. (previously presented) A computer program product according to claim 25, wherein name mappings justified by corresponding certificates are permitted in a said trust chain in addition to attribute delegations, and wherein seeking a backwards proof further comprises:

decomposing, as appropriate, a particular subgoal to be proved into a name mapping justified by an available certificate and a new subgoal corresponding to said particular subgoal but with the subject reverse mapped using said name mapping.

30. (previously presented) A computer program product according to any one of claims 25-29, wherein seeking a backwards proof further comprises:

maintaining a list of subgoals already generated and pursued, checking each new subgoal against said list, and terminating the process of seeking a backwards proof in failure in the event of a new subgoal being found to already exist in the list.

31. (currently amended) A computer program product according to any one of claims 25-29 ~~30~~, wherein at least some of said certificates used in proving a determined trust chain as found have associated validity data, the method further comprising traversing the trust chain in a forwards direction from the trusted attribute delegation that grounds it and combining the

validity data of all certificates involved to determine the validity of the overall attribute delegation represented by the chain.

32. (previously presented) A computer program product according to claim 19, wherein determining that a trust chain has been found comprises storing the state of the seeking of a backwards proof prior to checking the validity of the trust chain found, this state being used to continue the process should the check of the validity of the initially found chain show that the chain is not valid.

33. (currently amended) A computer program product according to any one of claims 25-29 ~~32~~, wherein an attribute-delegation certificate used to prove a said subgoal has a subject-directed condition associated with it requiring that a specified subject must have a particular attribute in order for the delegation to be valid, and wherein seeking a backwards proof further comprises:

making said subject-directed condition a further subgoal to be proved for the current chain being followed.

34. (previously presented) A computer program product according to claim 25, wherein the seeking of a backwards proof is run to completion to find all trust chains, if any, proving the primary goal.

35. (currently amended) A computer program product according to any one of claims 25-29 ~~30~~ and further for selecting certificates to be sent to a resource which requires proof that a subject has a particular attribute before allowing use of the resource, by:

finding a trust chain in respect of said subject and an issuer known, or likely, to be trusted by said resource; and

selecting for sending to said resource certificates associated with a trust chain, if any, thereby found.

36. (currently amended) A computer program product according to any one of claims 25-29 ~~30~~ and further for determining whether a resource requiring a user to have at least one predetermined attribute is usable by a subject presenting certificates to the resource, by:

finding a trust chain in respect of said subject and an issuer known and trusted by said resource; and

determining that use of the resource by the subject is permitted if a trust chain can be found.